Committee on
Homeland Security Democrats
Bennie G. Thompson, Ranking Member
www.house.gov/hsc/democrats/

May 26, 2005

Contact: Jennifer Porter Gore
Nadra Harrison
202.226.2616

Rep. Bennie G. Thompson Dismayed by Findings of a GAO Report on DHS Cybersecurity Protection Program

WASHINGTON—Rep. Bennie G. Thompson, Ranking Member, U.S. House Committee on Homeland Security, Thursday voiced concerns that the Department of Homeland Security (DHS) is bogged down by the wrong priorities and is unable to carry out its responsibility to improve the nation's cybersecurity infrastructure protections, which according to a Government Accountability Office (GAO) report released today the Department has failed to do.

DHS is responsible for 13 core cybersecurity areas. But the report, "Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities," finds the Department has been slow to develop a programmatic approach to cybersecurity. Specifically, GAO found that DHS has not developed a capacity to analyze computer-based threats, including developing a methodology, acquiring expertise, and obtaining infrastructure data. Yet, GAO urged DHS in 2001 to complete this process. Several factors have prevented the Department from establishing itself as the national focal point for cyberspace security including organizational instability, hiring and contracting issues, and a failure to effectively partner with federal, state and local governments and the private sector.

"This report lays out clearly what I and many of my colleagues have witnessed firsthand – the Administration has not done enough to build the Department of Homeland Security's credibility as **the** leader of our cybersecurity efforts," said Rep. Thompson.

GAO reports that critical infrastructure sectors, as well as localities, states, and the federal government face increasing cybersecurity threats. The report also finds that information attacks are more likely to threaten vital national interests and that the tools to launch cybersecurity attacks are becoming more easily available. When attackers target vulnerable computer systems they are able to exploit those vulnerabilities more quickly and effectively. For example, in March 2005, it was reported that hackers were targeting the U.S electric power grid and had gained access to U.S. utilities' electronic control systems.

"As long as the Department is not our nation's focal point for cybersecurity, our critical infrastructures remain largely unprepared or unaware of cybersecurity risks and how to respond to cyber emergencies. This is unacceptable as so much of our daily lives --from our banking to our water and electricity supplies—rely on a strong cyber infrastructure."

###